What is claimed is:

1. A logic circuit for performing modular multiplication of a first multi-bit binary value and a second multi-bit binary value, the logic circuit comprising:

input combination logic for receiving and combining the second multi-bit binary value and a group of W bits of the first multi-bit binary value every j^{th} input cycle to generate W multi-bit binary combination values every j^{th} input cycle, where the W bits comprise bits jW to (jW+W-1), W>1, j is the cycle index from 0 to k-1, k=N/W, and N is the number of bits of the first multi-bit binary value;

accumulator logic for holding a plurality of multi-bit binary values accumulated over previous cycles;

reduction logic for generating a W bit value Λ in a current cycle for use in the next cycle, for receiving a multi-bit modulus binary value, and for combining the multi-bit modulus binary value with a W bit value Λ generated in a current cycle to generate W multi-bit binary values for use in the next cycle;

combination logic connected to said input combination logic, said accumulator logic, and said reduction logic, and for combining the W multi-bit binary combination values generated by said input combination logic in the current cycle, the W multi-bit binary values generated by said reduction logic in the current cycle, and the multi-bit binary values held by said accumulator logic to generate a plurality of new multi-bit binary values for input to said accumulator logic to be held in the next cycle;

wherein said reduction logic is arranged to generate the W bit value Λ for the next cycle based on the multi-bit modulus binary value, the multi-bit binary values held in the accumulator logic, W multi-bit binary combination values generated by combination of the second multi-bit binary value and a group of W bits of the first multi-bit binary value in the current cycle, and the W bit value Λ generated for the current cycle.

2. A logic circuit according to claim 1, wherein said reduction logic is arranged to generate the W bit value Λ for the next cycle to make the W least significant bits of the plurality of new multi-bit binary values generated by the combination logic in the next

cycle zero, and said combination logic includes shift logic to shift the generated new multi-bit binary values by W bits before input to said accumulator logic.

3. A logic circuit according to claim 1, wherein said reduction logic is arranged to generate the W bit value Λ for the next cycle based on the 2W least significant bits of the multi-bit modulus binary value, the 2W least significant bits of the multi-bit binary values held in said accumulator logic in the current cycle, the jW to (jW+W-1) bits of the W multi-bit binary combination values generated by combination of the second multi-bit binary value and a group of W bits of the first multi-bit binary value in the current cycle, and the W bit value Λ generated by said generation logic for the current cycle.

4. A logic circuit according to claim 2, wherein said reduction logic is arranged to generate the W bit value Λ for the next cycle based on the 2W least significant bits of the multi-bit modulus binary value, the 2W least significant bits of the multi-bit binary values held in said accumulator logic in the current cycle, the jW to (jW+W-1) bits of the W multi-bit binary combination values generated by combination of the second multi-bit binary value and a group of W bits of the first multi-bit binary value in the current cycle, and the W bit value Λ generated by said generation logic for the current cycle.

5. A logic circuit according to claim 3, including pre-combination logic for receiving and combining the second multi-bit binary value and the jW to (jW+W-1) bits of the first multi-bit binary value in the current cycle to generate the W multi-bit binary combination values for input to said reduction logic for use in the next cycle.

6. A logic circuit according to claim 4, including pre-combination logic for receiving and combining the second multi-bit binary value and the jW to (jW+W-1) bits of the first multi-bit binary value in the current cycle to generate the W multi-bit binary combination values for input to said reduction logic for use in the next cycle.

7. A logic circuit according to claim 1, wherein said input combination logic is connected to said reduction logic to input the W multi-bit binary combination value to said reduction logic.

8. A logic circuit according to claim 1, wherein the reduction logic includes further input combination logic for receiving and combining the W multi-bit binary combination values in the current cycle to generate a single multi-bit binary combination value for use in the next cycle.

9. A logic circuit according to claim 1, wherein said combination logic is arranged to multiply the second multi-bit binary value and the group of W bits of the first multi-bit binary value every j^{th} input cycle to generate the W multi-bit binary combination values every j^{th} input cycle.

10. A logic circuit according to claim 9, wherein said combination logic comprises an array of AND logic gates.

11. A logic circuit according to claim 8, wherein said further input combination logic is arranged to multiply the second multi-bit binary value and the group of W bits of the first multi-bit binary value every j^{th} input cycle to generate the W multi-bit binary combination values every j^{th} input cycle.

12. A logic circuit according to claim 11, wherein said further input combination logic comprises an array of AND logic gates.

13. A logic circuit according to claim 5, wherein said pre-combination logic is arranged to multiply the second multi-bit binary value and the jW to (jW+jW-1) bits of the first multi-bit binary value in the current cycle to generate the W multi-bit binary combination values for input to the reduction logic for use in the next cycle.

14. A logic circuit according to claim 6, wherein said pre-combination logic is arranged to multiply the second multi-bit binary value and the jW to (jW+jW-1) bits of

the first multi-bit binary value in the current cycle to generate the W multi-bit binary combination values for input to the reduction logic for use in the next cycle.

15. A logic circuit according to claim 13, wherein said pre-combination logic comprises an array of AND logic gates.

16. A logic circuit according to claim 14, wherein said pre-combination logic comprises an array of AND logic gates.

17. A logic circuit according to claim 1, wherein said reduction logic is arranged to multiply the multi-bit modulus binary value with the W bit value Λ generated in a current cycle to generate W multi-bit binary values for use in the next cycle.

18. A logic circuit according to claim 17, wherein said reduction logic includes an array of AND gate logic for performing the multiplication.

19. A logic circuit according to claim 1, wherein said combination logic includes a plurality of parallel counters for performing the combination.

20. A logic circuit according to claim 19, wherein said parallel counters are arranged to each receive a corresponding bit of: the W multi-bit binary combination values generated by said input combination logic in the current cycle, the W multi-bit binary values generated by said reduction logic in the current cycle, and the multi-bit binary values held by said accumulator logic.

21. A logic circuit according to claim 19, wherein each parallel counter has (2W+R) inputs and R outputs, where R is the number of new multi-bit binary values input to said accumulator logic to be held in the next cycle.

22. A logic circuit according to claim 1, wherein said accumulator logic comprises an array of flip-flops, each flip-flop receiving a bit of one of the new multi-bit binary values output from said combination logic.

23. A logic circuit according to claim 1, wherein said reduction logic comprises high speed logic components to generate the W bit binary value Λ during the current cycle for use in the next cycle.

24. A logic circuit according to claim 1, wherein said reduction logic includes a plurality of parallel counters for generating the W bit binary value Λ.

25. A logic circuit according to claim 1, including final reduction logic for summing the plurality of new multi-bit binary values output from said combination logic at the end of the $(k-1)^{th}$ cycle and for subtracting the multi-bit modulus binary value from the sum if the sum is greater than or equal to the multi-bit modulus binary value.

26. A logic circuit according to claim 1, wherein the multi-bit modulus binary value is an odd number.

27. A logic circuit according to claim 1, wherein the logic circuit is arranged to perform Montgomery multiplication.

28. A logic circuit according to claim 1, wherein said input combination logic, said accumulator logic and said combination logic are formed of a plurality of logic elements, one for each input bit of the W multi-bit binary combination values.

29. A logic circuit according to claim 28, wherein said combination logic comprises a parallel counter in each said logic element.

30. A logic circuit according to claim 28, wherein said accumulator logic comprises an array of flip-flops in each said logic element.

31. A logic circuit according to claims 28, wherein said input combination logic comprises an array of AND gates in each logic element.

32. A logic circuit according to claim 28, wherein said logic elements comprise standard cells.

33. A logic circuit according to claim 1, including modulus modifying logic for initially modifying the multi-bit modulus binary value used by the logic circuit by a factor to make the W least significant bits ones.

34. A logic circuit according to claim 1, wherein said modulus modifying logic is arranged to initially modify the multi-bit modulus binary value to make the W to 2W-1 bits zeros.

35. A logic circuit according to claim 33 or claim 34, including final reduction logic for summing the plurality of new multi-bit binary values output from said combination logic at the end of the $(k-1)^{th}$ cycle, and for performing a function equivalent to comparing the sum and the multi-bit modulus binary value and, if the sum is greater or equal to the multi-bit modulus binary value, subtracting the multi-bit modulus binary value from the sum, and repeating the comparison and subtraction until the sum is less than the multi-bit modulus binary value.

36. A modular exponentiation logic circuit for performing modular exponentiation, comprising:

input logic for receiving a multi bit binary value to be exponentiated, a multi bit binary exponent, and a multi bit modulus binary value;

at least one logic circuit for performing modular multiplication of a first multi-bit binary value and a second multi-bit binary value, eahc logic circuit comprising:

input combination logic for receiving and combining the second multi-bit binary value and a group of W bits of the first multi-bit binary value every j^{th} input cycle to generate W multi-bit binary combination values every j^{th} input cycle, where the W bits comprise bits jW to (jW+W-1), W>1, j is the cycle index from 0 to k-1, k=N/W, and N is the number of bits of the first multi-bit binary value;

accumulator logic for holding a plurality of multi-bit binary values accumulated over previous cycles;

reduction logic for generating a W bit value Λ in a current cycle for use in the next cycle, for receiving a multi-bit modulus binary value, and for combining the multi-

bit modulus binary value with a W bit value Λ generated in a current cycle to generate W multi-bit binary values for use in the next cycle;

combination logic connected to said input combination logic, said accumulator logic, and said reduction logic, and for combining the W multi-bit binary combination values generated by said input combination logic in the current cycle, the W multi-bit binary values generated by said reduction logic in the current cycle, and the multi-bit binary values held by said accumulator logic to generate a plurality of new multi-bit binary values for input to said accumulator logic to be held in the next cycle;

wherein said reduction logic is arranged to generate the W bit value Λ for the next cycle based on the multi-bit modulus binary value, the multi-bit binary values held in the accumulator logic, W multi-bit binary combination values generated by combination of the second multi-bit binary value and a group of W bits of the first multi-bit binary value in the current cycle, and the W bit value Λ generated for the current cycle; and

said modular exponentiation logic circuit includes logic for inputting the multi bit binary number to be exponentiated and/or a multi bit binary number based on an output of at least one said logic circuit into at least one said logic circuit in dependence upon the multi bit binary exponent, and for forming a multi bit binary value comprising the modular exponentiation of the multi bit binary number to be exponentiated on the basis on an output of the or each said logic circuit.

37. A modular exponentiation logic circuit according to claim 36, wherein said reduction logic is arranged to generate the W bit value Λ for the next cycle to make the W least significant bits of the plurality of new multi-bit binary values generated by the combination logic in the next cycle zero, and said combination logic includes shift logic to shift the generated new multi-bit binary values by W bits before input to said accumulator logic.

38. A modular exponentiation logic circuit according to claim 36, wherein said reduction logic is arranged to generate the W bit value Λ for the next cycle based on the 2W least significant bits of the multi-bit modulus binary value, the 2W least significant bits of the multi-bit binary values held in said accumulator logic in the current cycle, the

jW to (jW+W-1) bits of the W multi-bit binary combination values generated by combination of the second multi-bit binary value and a group of W bits of the first multi-bit binary value in the current cycle, and the W bit value Λ generated by said generation logic for the current cycle.

39. A modular exponentiation logic circuit according to claim 38, including pre-combination logic for receiving and combining the second multi-bit binary value and the jW to (jW+W-1) bits of the first multi-bit binary value in the current cycle to generate the W multi-bit binary combination values for input to said reduction logic for use in the next cycle.

40. A modular exponentiation logic circuit according to claim 36, wherein said input combination logic is connected to said reduction logic to input the W multi-bit binary combination value to said reduction logic.

41. A modular exponentiation logic circuit according to claim 36, wherein the reduction logic includes further input combination logic for receiving and combining the W multi-bit binary combination values in the current cycle to generate a single multi-bit binary combination value for use in the next cycle.

42. A modular exponentiation logic circuit according to claim 36, wherein said combination logic is arranged to multiply the second multi-bit binary value and the group of W bits of the first multi-bit binary value every j^{th} input cycle to generate the W multi-bit binary combination values every j^{th} input cycle.

43. A modular exponentiation logic circuit according to claim 42, wherein said combination logic comprises an array of AND logic gates.

44. A modular exponentiation logic circuit according to claim 41, wherein said further input combination logic is arranged to multiply the second multi-bit binary value and the group of W bits of the first multi-bit binary value every j^{th} input cycle to generate the W multi-bit binary combination values every j^{th} input cycle.

45. A modular exponentiation logic circuit according to claim 44, wherein said further input combination logic comprises an array of AND logic gates.

46. A modular exponentiation logic circuit according to claim 39, wherein said pre-combination logic is arranged to multiply the second multi-bit binary value and the jW to (jW+jW-1) bits of the first multi-bit binary value in the current cycle to generate the W multi-bit binary combination values for input to the reduction logic for use in the next cycle.

47. A modular exponentiation logic circuit according to claim 46, wherein said pre-combination logic comprises an array of AND logic gates.

48. A modular exponentiation logic circuit according to claim 36, wherein said reduction logic is arranged to multiply the multi-bit modulus binary value with the W bit value Λ generated in a current cycle to generate W multi-bit binary values for use in the next cycle.

49. A modular exponentiation logic circuit according to claim 48, wherein said reduction logic includes an array of AND gate logic for performing the multiplication.

50. A modular exponentiation logic circuit according to claim 36, wherein said combination logic includes a plurality of parallel counters for performing the combination.

51. A modular exponentiation logic circuit according to claim 50, wherein said parallel counters are arranged to each receive a corresponding bit of: the W multi-bit binary combination values generated by said input combination logic in the current cycle, the W multi-bit binary values generated by said reduction logic in the current cycle, and the multi-bit binary values held by said accumulator logic.

52. A modular exponentiation logic circuit according to claim 50, wherein each parallel counter has (2W+R) inputs and R outputs, where R is the number of new multi-bit binary values input to said accumulator logic to be held in the next cycle.

53. A modular exponentiation logic circuit according to claim 36, wherein said accumulator logic comprises an array of flip-flops, each flip-flop receiving a bit of one of the new multi-bit binary values output from said combination logic.

54. A modular exponentiation logic circuit according to claim 36, wherein said reduction logic comprises high speed logic components to generate the W bit binary value Λ during the current cycle for use in the next cycle.

55. A modular exponentiation logic circuit according to claim 36, wherein said reduction logic includes a plurality of parallel counters for generating the W bit binary value Λ.

56. A modular exponentiation logic circuit according to claim 36, including final reduction logic for summing the plurality of new multi-bit binary values output from said combination logic at the end of the $(k-1)^{th}$ cycle and for subtracting the multi-bit modulus binary value from the sum if the sum is greater than or equal to the multi-bit modulus binary value.

57. A modular exponentiation logic circuit according to claim 36, wherein the multi-bit modulus binary value is an odd number.

58. A modular exponentiation logic circuit according to claim 36, wherein the logic circuit is arranged to perform Montgomery multiplication.

59. A modular exponentiation logic circuit according to claim 36, wherein said input combination logic, said accumulator logic and said combination logic are formed of a plurality of logic elements, one for each input bit of the W multi-bit binary combination values.

60. A modular exponentiation logic circuit according to claim 59, wherein said combination logic comprises a parallel counter in each said logic element.

61. A modular exponentiation logic circuit according to claim 59, wherein said accumulator logic comprises an array of flip-flops in each said logic element.

62. A modular exponentiation logic circuit according to claims 59, wherein said input combination logic comprises an array of AND gates in each logic element.

63. A modular exponentiation logic circuit according to claim 59, wherein said logic elements comprise standard cells.

64. A modular exponentiation logic circuit according to claim 36, including initial input logic for initially inputting a multi bit binary value $2^{2N}|$ mod m into at least one said logic circuit, where m is a multi bit binary modulus value and N is the number of bits of the multi bit binary value to be exponentiated.

65. A modular exponentiation logic circuit according to claim 64, wherein at least one said logic circuit is arranged to receive the multi bit binary value $2^{2N}|$ mod m and the multi bit binary value to be exponentiated as initial inputs.

66. A modular exponentiation logic circuit according to claim 65, wherein a said logic circuit is arranged to receive a final output of at least one said logic circuit and logic one as inputs to generate the multi bit binary value comprising the modular exponentiation of the multi bit binary number to be exponentiated.

67. A modular exponentiation logic circuit according to claim 36, including modulus modifying logic for initially modifying the multi-bit modulus binary value used by the modular exponentiation logic circuit by a factor to make the W least significant bits ones.

68. A modular exponentiation logic circuit according to claim 36, wherein said modulus modifying logic is arranged to initially modify the multi-bit modulus binary value to make the W to 2W-1 bits zeros.

69. A modular exponentiation logic circuit according to claim 67, including final reduction logic for modifying the multi bit binary value comprising the modular exponentiation of the multi bit binary number to be exponentiated to be less than the unmodified multi-bit modulus binary value.

70. A modular exponentiation logic circuit according to claim 68, including final reduction logic for modifying the multi bit binary value comprising the modular exponentiation of the multi bit binary number to be exponentiated to be less than the unmodified multi-bit modulus binary value.

71. A modular exponentiation logic circuit according to claim 69, wherein the final reduction logic is arranged to compare an output of at least one said logic circuit and the multi-bit modulus binary value and, if the output is greater or equal to the multi-bit modulus binary value, to subtract the multi-bit modulus binary value from the sum, and to repeat the comparison and subtraction until the output is less than the multi-bit modulus binary value.

72. A modular exponentiation logic circuit according to claim 70, wherein the final reduction logic is arranged to compare an output of at least one said logic circuit and the multi-bit modulus binary value and, if the output is greater or equal to the multi-bit modulus binary value, to subtract the multi-bit modulus binary value from the sum, and to repeat the comparison and subtraction until the output is less than the multi-bit modulus binary value.

73. An encryption logic circuit for encrypting or decrypting a multi-bit binary value comprising the logic circuit according to any claim 1 or claim 36.

74. An RSA encryption circuit for RSA encrypting or decrypting a multi-bit binary value comprising the logic circuit according to any claim 1 or 36.

75. An integrated circuit comprising the logic circuit according to claim 1 or 36.

76. An electronic device comprising the logic circuit according to claim 1 or 36.

77. A carrier medium carrying code defining characteristics of the logic circuit according to any one of claims 1 to 35.

78. A method of designing a logic circuit according to any one of claims 1 to 35, comprising implementing a computer program to generate information defining characteristics of the logic circuit.

79. A carrier medium carrying computer readable code for controlling a computer to implement the method of designing a logic circuit according to any one of claims 1 to 35 which comprises implementing a computer code to generate information defining characteristics of the logic circuit.

80. A design system for designing a logic circuit according to any one of claims 1 to 35, comprising a computer system for generating information defining characteristics of the logic circuit.

81. A method of manufacture of a logic circuit according to any one of claims 1 to 35, comprising designing and building the logic circuit in semiconductor material in accordance with code defining characteristics of the logic circuit.

82. A logic circuit for performing Montgomery multiplication between a first multi-bit binary value and a second multi-bit binary value, comprising:

input logic for inputting W multi-bit combination binary values comprised of the combination $X_{jW}Y_i$ to $X_{(jW+W-1)}Y_i$ of jW to (jW+W-1) bits of the first binary value X and i bits of the second multi-bit binary value, where j is the processing cycle from 0 to k-1, k=N/W, W>1, and N is the number of bits of the first multi-bit binary value;

accumulator logic for accumulating at least one multi-bit binary value A in a current cycle on the basis of multi-bit binary values in the accumulator in a previous cycle, and the input W multi-bit combination binary values; and

reduction logic for generating a W bit binary value Λ for a current cycle such that $\Lambda = A \mid \mathrm{mod} 2^W$, wherein said accumulator logic is arranged to update said at least one accumulated multi-bit binary value A for a current cycle by adding the product of

the generated W bit binary value Λ and a multi-bit binary modulus value and dividing the result by 2^W.

83. A logic circuit according to claim 82, including final reduction logic for determining a Montgomery product by subtracting the multi-bit binary modulus value from the accumulated multi-bit binary value or the sum of the accumulated multi-bit binary values if the accumulated multi-bit binary value or the sum of the accumulated multi-bit binary values is greater than or equal to the multi-bit binary modulus value.

84. A logic circuit according to claim 82, wherein said accumulator logic is arranged to accumulate said at least one multi-bit binary value A in a current cycle as $A + X_{jW}Y_i + 2X_{jW+1}Y_i + \ldots\ldots + 2^{W-1}X_{(jW+W-1)}Y_i$.

85. A logic circuit according to claim 82, wherein said reduction logic is arranged to determined the W bit binary value for the next cycle based on the W bit binary value for the current cycle, said at least one accumulated multi-bit binary value in said accumulator logic in the current cycle, the multi-bit binary modulus value, and the input W multi-bit combination binary values in the current cycle.

86. A logic circuit according to claim 83, wherein said reduction logic is arranged to determined the W bit binary value for the next cycle based on the W bit binary value for the current cycle, said at least one accumulated multi-bit binary value in said accumulator logic in the current cycle, the multi-bit binary modulus value, and the input W multi-bit combination binary values in the current cycle.

87. A logic circuit according to claim 82, wherein said reduction logic and said accumulator logic are arranged to operate in parallel during a cycle.

88. A modular exponentiation logic circuit for performing modular exponentiation, comprising:

input logic for receiving a multi bit binary value to be exponentiated, a multi bit binary exponent, and a multi bit modulus binary value; and

at least one logic circuit for performing Montgomery multiplication between a first multi-bit binary value and a second multi-bit binary value, each logic circuit comprising:

input logic for inputting W multi-bit combination binary values comprised of the combination $X_{jW}Y_i$ to $X_{(jW+W-1)}Y_i$ of jW to (jW+W-1) bits of the first binary value X and i bits of the second multi-bit binary value, where j is the processing cycle from 0 to k-1, k=N/W, W>1, and N is the number of bits of the first multi-bit binary value;

accumulator logic for accumulating at least one multi-bit binary value A in a current cycle on the basis of multi-bit binary values in the accumulator in a previous cycle, and the input W multi-bit combination binary values; and

reduction logic for generating a W bit binary value Λ for a current cycle such that $\Lambda = A \mid mod 2^W$, wherein said accumulator logic is arranged to update said at least one accumulated multi-bit binary value A for a current cycle by adding the product of the generated W bit binary value Λ and a multi-bit binary modulus value and dividing the result by 2^W.

89. A modular exponentiation logic circuit according to claim 88, including final reduction logic for determining a Montgomery product by subtracting the multi-bit binary modulus value from the accumulated multi-bit binary value or the sum of the accumulated multi-bit binary values if the accumulated multi-bit binary value or the sum of the accumulated multi-bit binary values is greater than or equal to the multi-bit binary modulus value.

90. A modular exponentiation logic circuit according to claim 88, wherein said accumulator logic is arranged to accumulate said at least one multi-bit binary value A in a current cycle as $A + X_{jW}Y_i + 2X_{jW+1}Y_i + \ldots\ldots + 2^{W-1}X_{(jW+W-1)}Y_i$.

91. A modular exponentiation logic circuit according to claim 88, wherein said reduction logic is arranged to determined the W bit binary value for the next cycle based on the W bit binary value for the current cycle, said at least one accumulated multi-bit binary value in said accumulator logic in the current cycle, the multi-bit binary modulus value, and the input W multi-bit combination binary values in the current cycle.

92. A modular exponentiation logic circuit according to claim 89, wherein said reduction logic is arranged to determined the W bit binary value for the next cycle based on the W bit binary value for the current cycle, said at least one accumulated multi-bit binary value in said accumulator logic in the current cycle, the multi-bit binary modulus value, and the input W multi-bit combination binary values in the current cycle.

93. A modular exponentiation logic circuit according to claim 88, wherein said reduction logic and said accumulator logic are arranged to operate in parallel during a cycle.

94. A modular exponentiation logic circuit according to claim 88, including modulus modifying logic for initially modifying the multi-bit modulus binary value used by the modular exponentiation logic circuit by a factor to make the W least significant bits ones.

95. A modular exponentiation logic circuit according to claim 94, wherein said modulus modifying logic is arranged to initially modify the multi-bit modulus binary value to make the 2W to 2W-1 bits zeros.

96. A modular exponentiation logic circuit according to claim 94, including final reduction logic for modifying the multi bit binary value comprising the modular exponentiation of the multi bit binary number to be exponentiated to be less than the unmodified multi-bit modulus binary value.

97. An encryption logic circuit for encrypting or decrypting a multi-bit binary value comprising the logic circuit according to any one of claims 82 to 96.

98. An RSA encryption circuit for RSA encrypting or decrypting a multi-bit binary value comprising the logic circuit according to claim 82.

99. An integrated circuit comprising the logic circuit according to claim 82.

100. An electronic device comprising the logic circuit according to claim 82.

101. A carrier medium carrying code defining characteristics of the logic circuit according to any one of claims 82 to 96.

102. A method of designing a logic circuit according to any one of claims 82 to 96, comprising implementing a computer program to generate information defining characteristics of the logic circuit.

103. A carrier medium carrying computer readable code for controlling a computer to implement the method of designing a logic circuit according to any one of claims 82 to 96 which comprises implementing the computer code to generate information defining characteristics of the logic circuit.

104. A design system for designing a logic circuit according to any one of claims 82 to 96, comprising a computer system for generating information defining characteristics of the logic circuit.

105. A method of manufacture of a logic circuit according to any one of claims 82 to 96, comprising designing and building the logic circuit in semiconductor material in accordance with the code defining characteristics of the logic circuit.

106. A logic circuit for performing modular multiplication, comprising:

a logic input for accessing combinations of two binary inputs to input W multi-bit binary combinations of two binary numbers, where W>1;

accumulator logic for accumulating multi-bit binary values;

combining logic for combining the input W multi-bit binary combinations and the values in the accumulator logic to generate new values for input to the accumulator logic; and

reduction logic for determining a W bit binary value A $|\text{mod } 2^W$, for receiving a multi-bit modulus binary value, and for generating W multi-bit binary values using the W bit binary value and the modulus binary value;

wherein said combination logic is arranged to generate the new values by also including the generated W multi-bit binary values.